IN THE CLAIMS

What is claimed is:

1. A computer software product including one or more recordable media having executable instructions stored thereon which, when executed by a processing device, causes the processing device to:

initialize a symbolic simulation relation for an assertion graph on a first symbolic lattice domain.

2. The computer software product recited in Claim 1 wherein initializing the symbolic simulation relation comprises causing the processing device to:

join a Boolean predicate for an outgoing edge from an initial vertex in the assertion graph with a symbolic antecedent labeling of an edge in the assertion graph.

3. The computer software product recited in Claim 2 wherein the symbolic antecedent labeling comprises a symbolic indexing function to encode a plurality of antecedent labels for a plurality of assertion graph instances, having at least one assertion graph instance on a second lattice domain different from the first symbolic lattice domain.

4. The computer software product recited in Claim 1 wherein the assertion graph on the first symbolic lattice domain is configurable to express a justification property to verify by computing the symbolic simulation relation.

5. The computer software product recited in Claim 4 which, when executed by a processing device, further causes the processing device to:

compute the symbolic simulation relation for the assertion graph on the first symbolic lattice domain; and

check the symbolic simulation relation to verify a plurality of properties

expressed by a plurality of assertion graph instances, having at least one assertion graph instance on a second lattice domain different from the first symbolic lattice domain.

6. The computer software product recited in Claim 1 which, when executed by a processing device, further causes the processing device to:

compute the symbolic simulation relation for the assertion graph on the first symbolic lattice domain; and

compare the symbolic simulation relation to a symbolic consequence labeling for the edge for the assertion graph on the first symbolic lattice domain.

7. The computer software product recited in Claim 6 wherein computing the symbolic simulation relation comprises causing the processing device to:

join the symbolic simulation relation for the assertion graph on the first symbolic lattice domain, to any states that are contained by a symbolic antecedent for a first plurality of edges of the assertion graph on the first symbolic lattice domain and also contained by a symbolic post-image for a second plurality of edges incoming to the first plurality of edges.

8. The computer software product recited in Claim 1 which, when executed by a processing device, further causes the processing device to:

compute the symbolic simulation relation for the assertion graph on the first symbolic lattice domain to verify the assertion graph according to a normal satisfiability criteria.

9. A method comprising:

initializing a symbolic simulation relation for an assertion graph on a first symbolic lattice domain.

10. The method recited in Claim 9 wherein initializing the symbolic simulation relation comprises:

joining a Boolean predicate for an outgoing edge from an initial vertex in the assertion graph with a symbolic antecedent labeling of an edge in the assertion graph.

11. The method recited in Claim 10 wherein the symbolic antecedent labeling comprises a symbolic indexing function to encode a plurality of antecedent labels for a plurality of assertion graph instances, having at least one assertion graph instance on a second lattice domain different from the first symbolic lattice domain.

12. The method recited in Claim 9 further comprising:

computing the symbolic simulation relation for the assertion graph on the first symbolic lattice domain; and

comparing the symbolic simulation relation to a symbolic consequence labeling for the edge for the assertion graph on the first symbolic lattice domain.

13. The method recited in Claim 12 wherein computing the symbolic simulation relation comprises:

joining the symbolic simulation relation for the assertion graph on the first symbolic lattice domain, to any states that are contained by a symbolic antecedent for a first plurality of edges of the assertion graph on the first symbolic lattice domain and also contained by a symbolic post-image for a second plurality of edges incoming to the first plurality of edges.

14. The method recited in Claim 9 wherein the assertion graph on the first symbolic lattice domain is configurable to express a justification property to verify through computing the symbolic simulation relation.

15. The method recited in Claim 14 further comprising:

computing the symbolic simulation relation for the assertion graph on the first symbolic lattice domain; and

checking the symbolic simulation relation to verify a plurality of properties expressed by a plurality of corresponding assertion graph instances, having at least one assertion graph instance on a second lattice domain different from the first symbolic lattice domain.

16. A method comprising:

specifying a justification property with an assertion graph.

17. The method recited in Claim 16 wherein the assertion graph is on a first symbolic lattice domain; and the justification property is expressed by one of a plurality of instances of the assertion graph, at least one assertion graph instance on a second lattice domain different from the first symbolic lattice domain.

18. The method recited in Claim 17 further comprising:

computing a symbolic simulation relation for the assertion graph on the first symbolic lattice domain; and

checking the symbolic simulation relation with a symbolic consequence labeling for the assertion graph on the first symbolic lattice domain according to a normal satisfiability criteria.

19. A method comprising:

merging a plurality of properties in an assertion graph on a first symbolic lattice domain by using a symbolic labeling.

20. The method recited in Claim 19 wherein the symbolic labeling comprises a symbolic indexing function to encode a plurality of labels for a plurality of

assertion graph instances, having at least one assertion graph instance on a second lattice domain different from the first symbolic lattice domain.

21. A formal verification method comprising:

defining an assertion graph including an antecedent label and a consequence label;

simulating a finite state system having an initial state condition or an input to generate a subsequent state condition or an output;

comparing the initial state condition or the input to any antecedent along an infinite transition path through the assertion graph to identify any antecedent violation; and

comparing the subsequent state condition or the output to the consequence if no antecedent violation was identified.

22. A verification system comprising:

means for initializing a symbolic simulation relation for an assertion graph on a first symbolic lattice domain.

23. The verification system of Claim 22 wherein the means for initializing the symbolic simulation relation comprises:

means for joining a Boolean predicate for an outgoing edge from an initial vertex in the assertion graph with a symbolic antecedent labeling of an edge in the assertion graph.

24. The verification system of Claim 23 wherein the symbolic antecedent labeling comprises a symbolic indexing function to encode a plurality of antecedent labels for a plurality of assertion graph instances, having at least one assertion graph instance on a second lattice domain different from the first symbolic lattice domain.

25. The verification system of Claim 22 further comprising:

means for computing the symbolic simulation relation for the assertion graph on the first symbolic lattice domain; and

means for comparing the symbolic simulation relation to a symbolic consequence labeling for the edge for the assertion graph on the first symbolic lattice domain.

26. The method recited in Claim 25 wherein the means for computing the symbolic simulation relation comprises:

means for joining into what is already contained by the symbolic simulation relation for the assertion graph on the first symbolic lattice domain, any states that are contained by a symbolic antecedent for a first plurality of edges of the assertion graph on the first symbolic lattice domain and also contained by a symbolic post-image for a second plurality of edges incoming to the first plurality of edges.

27. The verification system of Claim 9 wherein the assertion graph on the first symbolic lattice domain is configurable to express a justification property to verify through computing the symbolic simulation relation.

28. The verification system of Claim 27 further comprising:

means for computing the symbolic simulation relation for the assertion graph on the first symbolic lattice domain; and

means for checking the symbolic simulation relation to verify a plurality of properties expressed by a plurality of corresponding assertion graph instances, having at least one assertion graph instance on a second lattice domain different from the first symbolic lattice domain.

29. A verification system comprising:

means for specifying a justification property with an assertion graph.

30. The verification system of Claim 29 wherein the assertion graph is on a first symbolic lattice domain; and the justification property is expressed by one of a plurality of instances of the assertion graph, at least one assertion graph instance on a second lattice domain different from the first symbolic lattice domain.